4 PERFORM SYSTEM ENGINEERING

4.1 System Engineering

The Federal Aviation Administration (FAA) System Engineering (SE) method is robust, iterative, and has extensive interdependencies among the SE elements listed in Table 1.2-1. The process workflow (see Figure 4.1-1) captures the essence of these linkages and provides a high-level view of the various SE processes and how they functionally interact. These functional interfaces only represent the predominant interaction between each process. The interaction between processes at a lower level is much more involved (i.e., Figure 4.1-1 is a simplified view and does not depict all the ways that processes interface). Figure 3.1-2 is an N^2 diagram of SE that shows the actual work products exchanged between the various SE processes shown in Figure 4.1-1.

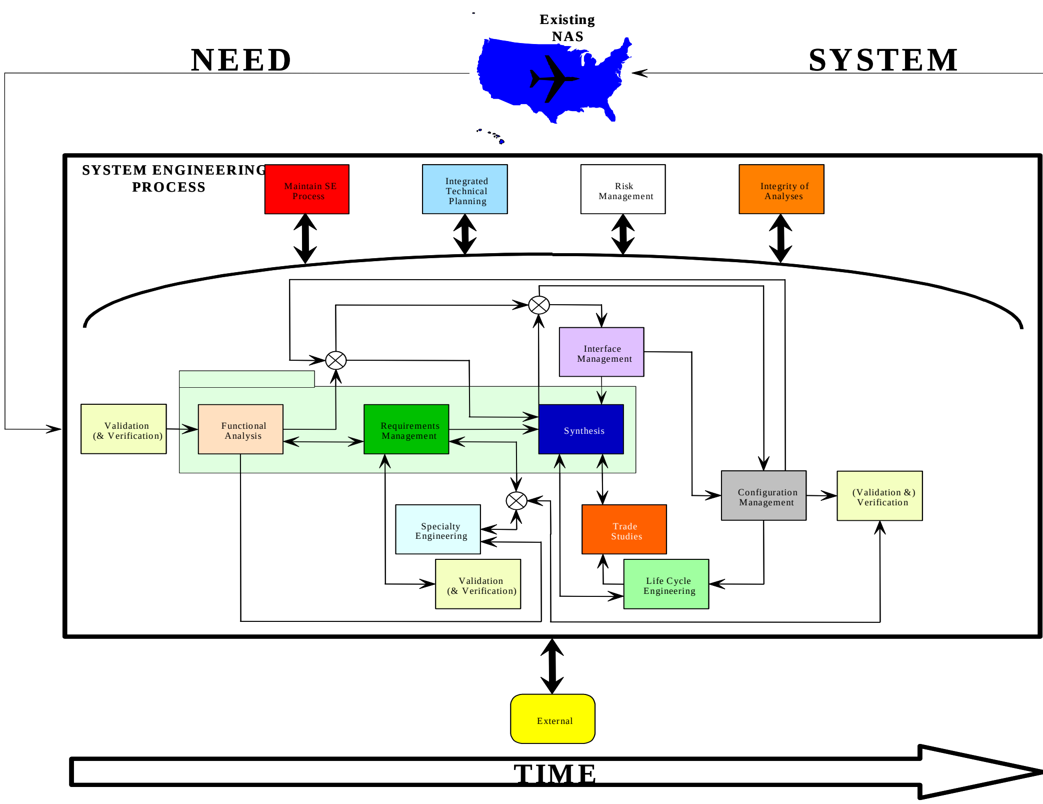

Figure 4.1-1. Functional Flow Diagram of System Engineering

In Figure 4.1-1, each SE process is laid out from left to right to notionally depict when in time each process is employed relative to another. The time arrow is *not* relative to the AMS lifecycle phases. It is recommended to note that overall SE, and many of the interactions at the lower levels, may be iterative in nature; thus, the left to right timeline is notional.

Figure 4.1-1 indicates that SE is initiated when there is a need; that is, a recognized shortfall in capability within the NAS. For example, the stakeholder need may arise as a result of a new service to be provided or with the advent of technological innovations to be leveraged to reap improvements in capacity, security, and/or safety. Once the need is validated, the Functional Analysis process (Section 4.4) is performed to develop a Concept of Operations (CONOPS).

The Requirements Management process (Section 4.3) uses the CONOPS to develop an MNS, which is then fed back to Functional Analysis as input to develop the highest level of functional architecture for the new or modified system. The Requirements Management process uses this high-level functional architecture, as well as inputs from Specialty Engineering analyses, to develop requirements. These requirements are validated via the Validation and Verification process (Section 4.12). The interaction between Functional Analysis and Requirements Management is iterative, as the functional architecture and resulting requirements are decomposed to a level necessary to the appropriate requirements that describe the needed system characteristics. Synthesis (Section 4.5) then develops the physical architecture or design solution to those requirements.

Along with these initial SE activities, three overarching processes that interact with all SE processes are employed. These overarching processes continue throughout the system's lifecycle and are as follows:

- Integrated Technical Planning (Section 4.2)
  - Provides the technical guidance tools required to track and manage program activity
- Risk Management (Section 4.10)
  - Provides an organized, systematic decision-making approach to identify risks that affect achievement of program goals
  - Analyzes identified risks
  - Mitigates risks effectively
  - Tracks the progress of the mitigation efforts
- Integrity of Analyses (Section 4.9)
  - Ensures the provision of credible, useful, and sufficient data/results for program management's decision-making process
  - Ensures the integrity and fidelity of the various analysis tools

Once a valid set of requirements is obtained, the Synthesis process (Section 4.5) is initiated to define system elements and to refine and integrate these elements into a physical architecture. In addition to the requirements input into the Synthesis process, the functional architecture is provided to clarify and bound the system. The Trade Studies process (Section 4.6) and the Lifecycle Engineering process (Section 4.13) supply cost estimates to support the Synthesis process, which ultimately determines the design alternative that best satisfies the identified stakeholder need.

Interface Management (Section 4.7) plays a key role in ensuring that the various internal system pieces are coordinated as well as integrated with external systems. As the total system is decomposed via iterative interaction of Functional Analysis, Requirements Management, and Synthesis, physical and functional interfaces are identified and managed.

The results of these SE activities are continually brought under Configuration Management (Section 4.11). The system is developed according to the baseline design and verified with the Validation and Verification process (Section 4.12). With the system verified as able to meet the identified stakeholder need, it is deployed into the NAS. Although the discussion of this simplified view and description of SE was sequential, SE is truly iterative and employed continuously throughout the lifecycle of the system.

When used properly, SE creates an infrastructure that ensures customer requirements and expectations are effectively and efficiently identified, integrated, and managed. Each SE element is designed to maximize the thoroughness and quality of interaction and cooperation between individuals, teams, suppliers, and stakeholders as each SE element is performed. In addition, each SE element plays various roles throughout the lifecycle phases as shown in Figure 3.2-1. The summary provided below gives an overview of each SE element in terms of objective, definition, and value. Each SE element is extensively documented in the subsequent sections (Sections 4.2 through 4.14), which contain the following details:

- Process-Based Management (PBM) chart (objectives, inputs and associated providing process (providers), outputs and associated receiving process (customers), process tasks, and applicable lifecycle phases)
- Process workflow
- Methods, tools, and detailed descriptions of how each SE element's tasks are accomplished
- Steps to tailor the SE element
- Appendices for terms, acronyms, and work product examples

4.1.1 Summary of System Engineering Areas

The following paragraphs briefly summarize FAA SE and its 13 elements. The subsequent sections of the System Engineering Manual (SEM) further detail each element. The brackets following each subsection heading provide a cross-reference to the applicable section number and the relevant integrated Capability Maturity Model (iCMM) process areas.

4.1.1.1 System Engineering

[SEM 4.1; iCMM PA 01 through 04, 07, 08, 11, 13, 16, 20, and 21]

4.1.1.1.1 Objective

The objective of SE within the FAA is to consistently provide balanced solutions to complex FAA system needs.

4.1.1.1.2 Definition

SE defines how the organization discerns a problem, how it approaches solution development to a problem, and how it implements the plan enabling resolution of the problem. It is a discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all facets and variables and relating the social aspects to the technical aspects.

4.1.1.1.3 Utilization and Value

While SE process elements support the cycle defined by the Acquisition Management System (AMS), they also provide more granularity. This finer, more detailed breakdown provides better management visibility into the operation of the program. Risk is reduced through earlier identification of issues and better identification of requirements. Cost is reduced through earlier recognition and correction of problems. Support organizations are able to gauge and plan their work to support each phase.

4.1.1.2 Integrated Technical Planning

[SEM 4.2; iCMM PA 11]

4.1.1.2.1 Objective

The objective of the Integrated Technical Planning element (Section 4.2) is to provide program management with a sound, repeatable method for the execution of a requirements-based and structurally managed program.

4.1.1.2.2 Definition

The Integrated Technical Planning element provides program management with specific guidance and direction on how to plan a program's execution. The technical plans provide stakeholder- and contract-driven tailoring of SE to optimally satisfy program needs. These plans are living documents that are kept current throughout the program's lifecycle.

4.1.1.2.3 Utilization and Value

Various levels of technical and program management use the technical plans that result from Integrated Technical Planning. Expending upfront effort to generate clear, complete, and correct technical plans results in consistent performance across the program. Optimally, miscommunication and misinterpretation of stakeholder and executive expectations by individuals are eliminated. Developing and following properly prepared plans assists in eliminating miscommunication and helps the program to adapt to changes in program environment.

4.1.1.3 Requirements Management

[SEM 4.3; iCMM PA 01 and 02]

4.1.1.3.1 Objective

The objective of the Requirements Management element (Section 4.3) is to identify and develop all requirements and ensure that they are met throughout the product's lifecycle.

4.1.1.3.2 Definition

The Requirements Management element is a series of iterative tasks performed by a multifunction team throughout all AMS phases. The team's focus is to elicit, develop, manage, and control requirements and associated documentation. Once requirements are defined, the team uses a disciplined Requirements Management methodology to manage the requirements through verification, helping to ensure compliance with stakeholder needs and expectations, communication of allocations, and adaptation to/control of changes.

4.1.1.3.3 Utilization and Value

Requirements are the fuel for the design process. They define the needed characteristics of a system at all levels of complexity. They are derived from multiple inputs from internal and external sources that need to be logically and efficiently collected and synthesized in a centralized, accessible decision database(s). The information collected, managed, and controlled is accessed by various teams within the stakeholder and program organizations, associated internal interfaces (e.g., management or operations), and contractors/suppliers. When Requirements Management is performed well, rework and poorly communicated information typically is minimal, if not eliminated entirely. Furthermore, this process is used to surface gaps, redundancies, biases, and/or inconsistencies and resolve, revise, and/or refine them in a consistent, integrated method to the satisfaction and agreement of all the stakeholders. The solid foundation built through Requirements Management provides an ongoing resource for all program stages.

4.1.1.4 Functional Analysis

[SEM 4.4; iCMM PA 03]

4.1.1.4.1 Objective

The objective of the Functional Analysis element (Section 4.4) is to provide a framework for requirements that significantly improves innovation, synthesis, and product integration.

4.1.1.4.2 Definition

The Functional Analysis element takes the stakeholders' needs and translates them into a sequenced and traceable functional architecture. The system is represented as a set of functions defined as tasks, actions, or activities that are performed to achieve specified sequenced and time-based behaviors. Functions are described as what needs to be done, not how. Therefore, each function is written in the verb-noun form (e.g., “read book” and “cook food”). The functions are accomplished by one or more elements, including equipment/hardware, software, firmware, facilities, personnel, and/or procedural data. Each function is hierarchically decomposed until the basic subfunction is reached, and the requirements are fully developed. The functional architecture defines what the system does, including interfaces (both within the system and to the external world).

4.1.1.4.3 Utilization and Value

A logically sequenced and thoroughly functional architecture is critical to the definition of requirements. It surfaces innovative design solutions and sheds light on vague interfaces. It also provides the basis for logical and realistic product integration and synthesis. As the analyses are performed, additional requirements often are flushed out/derived, thereby providing the program with a more detailed list of requirements and an increased understanding of the system. The functional architecture and functional interfaces enable the stakeholders and program management to logically develop requirements down to the lowest level of a system hierarchy.

4.1.1.5 Synthesis

[SEM 4.5; iCMM PA 04]

4.1.1.5.1 Objective

The objective of the Synthesis element (Section 4.5) is to develop (synthesize) balanced solutions to requirements.

4.1.1.5.2 Definition

The Synthesis element develops solutions to problems (as defined by the requirements). This SE element uses scientific/engineering knowledge and methods to derive and document the hows used to solve the whats that are reflected in the requirements. The synthesized design generated is a balanced (i.e., cost, quality, schedule, risk, performance, producible/supportable) solution. The synthesized design is created through the analysis of candidate elements. The candidate elements are preliminarily defined and then iterated until the refinement of the system concept is complete. The final outputs, which also show relationships between candidate elements, are distributed to the groups responsible for building various system elements.

4.1.1.5.3 Utilization and Value

A series of benchmarks for various design performance parameters (e.g., power, data storage, testability, reliability) are generated and used to measure the viability and worth of a candidate design solution. Design performance parameters, ranked by importance, are refined during the design evolution of an affordable, responsive system design. Throughout the evolutionary analyses, credibility and acceptability by the stakeholders shall be ensured. The iterative nature of the candidate element task provides the mechanism for continuous correction of design inadequacies and refinement of the physical allocation process. It also surfaces opportunities for new technologies and innovative ideas to be considered, justified, and integrated. These efforts are used to validate the synthesized design in terms of balance, completeness, understandability, and reflection of the stakeholders' requirements.

4.1.1.6 Trade Studies

[SEM 4.6; iCMM PA 04]

4.1.1.6.1 Objective

The objective of the Trade Studies element (Section 4.6) is to select balanced (i.e., cost, schedule, quality, and risk) solutions from a set of available alternatives based on defined criteria.

4.1.1.6.2 Definition

The Trade Studies element is used by multidisciplinary teams to confirm that the most balanced technical solutions have been identified. The team methodically evaluates a series of design alternatives and recommends the preferred feasible solutions that enhance the value and performance of the overall system and/or functions. The primary assessment methods are the +/- method, the weighted value method, and the cost assessment method. Each assessment is taken to an appropriate level of detail that allows differentiation between alternatives. Recommendations are assembled in a trade study report and forwarded to the appropriate decisionmaker(s) (e.g., program management or stakeholders) for action.

4.1.1.6.3 Utilization and Value

The tasks within the Trade Studies element are designed to assist decisionmakers. The thorough identification and assessment of multiple facets of a problem aids the decisionmaker to relate the whole problem to optimal, feasible solutions by comparing technical, cost, and schedule interactions. The appropriate authority uses this information to make a final decision. The Trade Studies process provides the traceability needed to substantiate design and configuration changes to the baseline product design; it also documents why one alternative was chosen over another during the decisionmaking process.

4.1.1.7 Interface Management

[SEM 4.7; iCMM PA 07]

4.1.1.7.1 Objective

The objective of the Interface Management element (Section 4.7) is to achieve functional and physical compatibility between all interrelated system elements.

4.1.1.7.2 Definition

An interface is any boundary between one area and another. It may be external, internal, functional, or physical. Interfaces occur within the system (internal) as well as between the instant system and another system (external) and may be functional or physical (e.g., mechanical, electrical) in nature. Interface requirements are documented in an Interface Requirements Document (IRD). The Interface Control Document (ICD) contains the final details of how the contractor implements the requirements. An Interface Control Plan describes the management process for IRDs and ICDs. This plan provides the means to identify and resolve interface incompatibilities and to determine the impact of interface design changes.

4.1.1.7.3 Utilization and Value

During the program's life, compatibility and accessibility shall be maintained for the many diverse elements. Compatibility analysis of the interface definition demonstrates completeness of the interface and traceability records (or lack thereof). As changes are made, an authoritative means of controlling the design of interfaces shall be managed with appropriate documentation, thereby avoiding the situation in which hardware/software, when integrated into the system, fails to function as part of the system, as intended. Ensuring that all system pieces work together is a complex task that involves teams, stakeholders, contractors, and program management from the end of the initial concept definition stage through the operations and support stage.

4.1.1.8 Specialty Engineering

[SEM 4.8; iCMM PA N/A]

4.1.1.8.1 Objective

The objective of the Specialty Engineering element (Section 4.8) is twofold: (1) to integrate specific system attributes and disciplines into the acquisition process; and (2) to assess and confirm various system attributes (Specialty Engineering).

4.1.1.8.2 Definition

The Specialty Engineering element includes System Safety Engineering (SSE); Reliability, Maintainability, and Availability (RMA); Human Engineering (human factors); Electromagnetic Environmental Effects (E^3); Quality Engineering; Information Security Engineering; and Hazardous Materials Management/Environmental Engineering. Specialty Engineering analyses describe technical details of the design from a particular perspective and often require specialized skills. These analyses help the program to define requirements and design features and/or describe characteristics of the design and related operations in support of Validation and Verification (Section 4.12), requirements, Trade Studies (Section 4.6), Synthesis (Section 4.5), and Functional Analysis (Section 4.4). These analyses are performed throughout the product's lifecycle. At minimum, analysis results shall be available at standard design milestones, including the preliminary and critical design reviews. Table 4.1-1 provides a general description of the specialty engineering disciplines.

Table 4.1-1. Specialty Engineering Disciplines

Specialty Engineering Discipline	Description
SSE	Evaluation and management of the safety risk associated with a system using measures of safety risk identified in various hazard analyses, fault tree analyses, safety risk assessments, and hazard tracking and control.
RMA	Quantitative and qualitative analyses of the attributes of the system to perform reliably. Quantitative assessments are in the form of probabilistic, mean, and/or distribution assessments. Qualitative analyses are in the form of failure mode assessments. Evaluation of the design's ability to meet operational readiness requirements through preventive and corrective maintenance.
Human Factors Engineering	Human factors is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: – equipment, systems, facilities – procedures, jobs, environments – staffing – training – personnel and organizational management for safe, comfortable, and effective human performance.

Specialty Engineering Discipline	Description
E^3	Analysis of the system for susceptibility and/or vulnerability to electromagnetic fields or capability to generate such fields that might interfere with other systems, identify sources of interference, and means for correction within the levels prescribed by law, program requirements, spectrum management, or recognized standards. E^3 is composed of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC)
Quality Engineering	Evaluation of a system's ability to meet its requirements and to mitigate product defects.
Information Security Engineering	Evaluation of the vulnerability of the system to unauthorized access and use, or susceptibility to sabotage. Assessment of the ability of the system to survive a security threat in the expected operational environment.
Hazardous Materials Management/Environmental Engineering	Determination of environmental impacts at deployment sites and during operations, including both environmental impacts on the system and system impacts on the environment during all phases of the product life.

4.1.1.8.3 Utilization and Value

These analyses are used to support functional analysis, define and allocate requirements, contribute to the design, and to evaluate design progress, technical soundness, and risk. They are also needed by the stakeholders to ensure that the product performs as intended, as well as by engineering, operations, and product support personnel to accomplish their responsibilities in product development and operation.

4.1.1.9 Integrity of Analyses

[SEM 4.9; iCMM PA N/A]

4.1.1.9.1 Objective

The objective of the Integrity of Analyses element (Section 4.9) is to ensure that analyses provide the required level of fidelity and accuracy in a timely manner.

4.1.1.9.2 Definition

Throughout SE and the program's lifecycle, analyses are constantly being performed. These analyses range from simple to complex, quantitative to qualitative, top-down to bottom-up, and basic formulas to sophisticated simulations. In order to ensure credible, useful, and sufficient data/results for program management's decisionmaking process, the integrity and fidelity of the various analysis tools shall be understood and validated. This validation takes several forms: the attributes of the tool suite, validity of the input data, and proficiency and workmanship of the analyst. An Analysis Management Plan is generated that outlines the details of the various analysis methods and tools. It is recommended that this plan also reflect the program's constraints in terms of technical capabilities, schedule requirements, and cost requirements.

4.1.1.9.3 Utilization and Value

The initial selection of the method, tools, or model to be used in an analysis focuses on determining a practical tool that provides the most visibility into the problem with the least complexity. Because this process is iterative, there is an ongoing need to use the best approach to select the right method, tool, or model, considering the preferences of the stakeholders, other teams' previous experience with different tools, and the limitations of budgets, technology, and schedule. The bottom line is to have analyses in place that guard against mistakes and embed a consistent level of confidence in the integrity of the analysis. The analysis, in turn, contributes significantly to the success of the decisionmaking processes of program management, teams, stakeholders, and contract managers.

4.1.1.10 Risk Management

[SEM 4.10; iCMM PA 13]

4.1.1.10.1 Objective

The objective of the Risk Management element (Section 4.10) is to identify and analyze the uncertainties of achieving program objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

4.1.1.10.2 Definition

The Risk Management element is an organized, systematic decisionmaking SE process element used by all disciplines and program teams to identify risks regarding achieving program goals, analyze these risks, and effectively mitigate these risks. Risk is defined as an event or situation with a realistic uncertainty of occurrence and an unfavorable consequence if the risk occurs. Risk Management is applied at all levels, from small projects to large programs. Risks are identified (what might go wrong), impacts are analyzed (how big is the risk), mitigation plans are defined (how to reduce the risk), and risk status is continuously tracked and monitored (how the mitigation efforts are progressing). Identifying risks begins when a program is initiated and continues throughout the program's life. A risk watchlist, which compiles the most significant risk items into a single composite document, is generated. The watchlists are used to continuously monitor and track the overall risk status within team meetings and program management reviews.

4.1.1.10.3 Utilization and Value

Understanding the levels of likelihood and consequences of risk occurring increases the program manager's and program team's ability to anticipate and control the impacts of internal and/or external events on their programs. These impacts include, but are not limited to, cost, quality, schedule, and stakeholder satisfaction trends. The comprehensiveness of the analysis drives the thoroughness of what resources are required to mitigate the risk (e.g., budgets, requirements changes, stakeholder interfaces). Risk identification worksheets, tools, and terminology ensure a consistent approach that generates an analysis in which subjectivity is minimized, and confidence in the analysis is maximized.

4.1.1.11 Configuration Management

[SEM 4.11; iCMM PA 16]

4.1.1.11.1 Objective

The objective of the Configuration Management element (Section 4.11) is to establish and maintain consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

4.1.1.11.2 Definition

The Configuration Management element is an orderly identification, documentation, and maintenance of a product's functional performance and physical attributes. The tasks are focused on consistency of requirements, design, and operational information throughout the product's life. Once baselined as defined by stakeholder requirements, changes are systematically approved and managed to ensure that traceability/accountability is maintained throughout myriad levels of documentation. The scope of this process element begins with planning the Configuration Management process for the context and environment in which it is to be performed. It ends when the configuration and its associated changes are verified and audited for accuracy and completeness. Throughout the entire Configuration Management effort, a status check provides accurate and timely information concerning the product and its associated data. Support tasks within Configuration Management include developing training plans, defining performance-based management measurements, and assessing methods and trends to effect process improvements.

4.1.1.11.3 Utilization and Value

Configuration Management benefits the program, stakeholders, and contractors/suppliers. As product attributes are defined, measurable performance parameters may be established for the product's acquisition and use. As changes are made, Configuration Management provides correct and current information to the decisionmaking process. When configurations are managed, product repeatability is enhanced, guesswork and downstream surprises are avoided, cost and schedule savings are realized, erratic changes are minimized, proper replacement and repairs are ensured, and maintenance costs are reduced. The overall effect is the establishment of a high level of confidence in the product information.

4.1.1.12 Validation and Verification

[SEM 4.12; iCMM PA 08]

4.1.1.12.1 Objective

The objective of the Validation and Verification element (Section 4.12) is to determine that the system and process requirements are correct and have been met.

4.1.1.12.2 Definition

The Validation and Verification element ensures that all system requirements are correct and have been met. The Validation process proves requirements are correct. The Verification process proves that requirements are met. Requirements may not be verified by test alone.

The majority of requirements are verified by a combination of test and assessment, which comprise the two categories of verification. Test is the disciplined and controlled subjection of the system to conditions that replicate operations in a real or simulated environment as defined by the requirements. It involves examination, observation, and evaluation of measurable parameters of a system element. Assessment, the second category of verification, includes analysis, demonstration, inspection, verification by similarity, validation of records, simulation, and review of design documentation. It is a basic principle of SE that all requirements shall be verified.

4.1.1.12.3 Utilization and Value

The Validation process eliminates poor or unnecessary requirements, ensuring that the FAA obtains a set of requirements that are necessary and sufficient to meet the needs of the stakeholders. The Verification process ensures that the product satisfies the validated requirements, and thus meets the stakeholders' needs.

4.1.1.13 Lifecycle Engineering

[SEM 4.13; iCMM PA N/A]

4.1.1.13.1 Objective

The objective of the Lifecycle Engineering element (Section 4.13) is to assess and confirm system attributes (Lifecycle Engineering).

4.1.1.13.2 Definition

The Lifecycle Engineering analyses supplement the program to define requirements and design features or describe characteristics of the design and related operations. These analyses provide technical details of the design from a particular perspective and are performed throughout the product's lifecycle. At minimum, analysis results shall be available at standard design milestones, including the preliminary and critical design reviews.

4.1.1.13.3 Utilization and Value

These analyses are used to evaluate design progress, technical soundness, and risk. They are also needed by the stakeholders to ensure that the product performs as intended, as well as by engineering, operations, and product support personnel to accomplish their responsibilities in product development and operation.

4.1.1.14 System Engineering Process Management

[SEM 4.14; iCMM PA 20 & 21]

4.1.1.14.1 Objective

The System Engineering Process Management element (Section 4.14) has two objectives. The first is to manage and maintain the SE processes in order to satisfy the FAA's goals. This objective is accomplished by maintaining technical awareness, inserting new technology into SE, maintaining the SE support environment, and monitoring the SE support environment for improvement opportunities. The second is to gain agencywide skill and process consistency by continuously improving the effectiveness and efficiency of the SE processes. This objective is accomplished by analyzing the processes and explicitly planning and deploying improvements to those processes.

4.1.1.14.2 Definition

System Engineering Process Management provides support and balance for the 12 other SE process elements. It also covers activities to measure and improve the SE process elements, which involves designing, developing, improving, and maintaining definitions of SE activities, work, products, methods, techniques, practices, and tools. It additionally provides the technology environment needed to develop systems and perform SE.

4.1.1.14.3 Utilization and Value

This process provides the details and data required to ensure and improve the efficiency and effectiveness of overall SE. In turn, the purpose of improved SE is to reduce cost and schedule, while improving the efficiency and safety of the National Airspace System.